Randhir Pratap Singh

Batch- 19

3-Tier Architecture using NSG, ASG with NGINX, Tomcat, and *MySQL*

First we create

Step 1 - Resource group

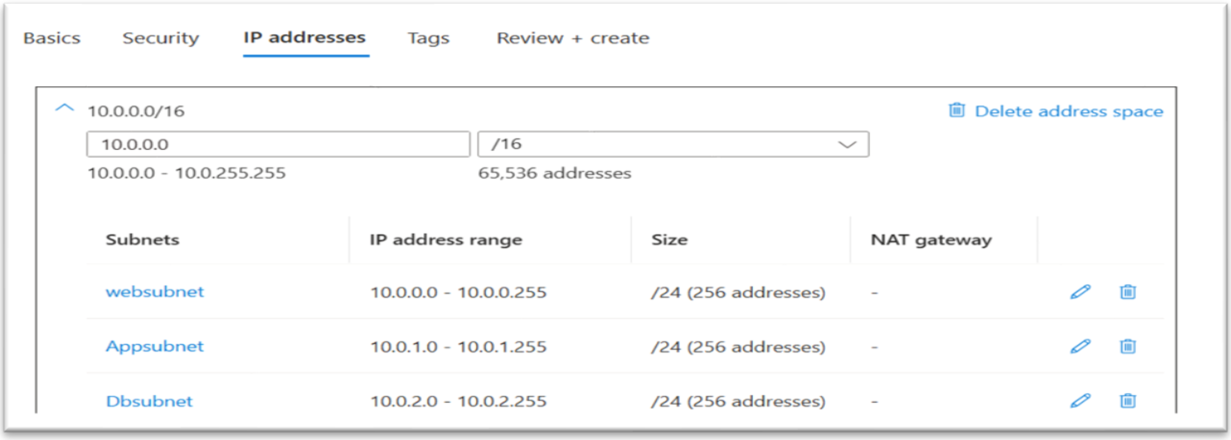
Step 2 - Virtual network in same region

In virtual network we create 3 subnets

* WebSubnet (for Web Server): 10.0.0.0/24

* AppSubnet (for App Server): 10.0.1.0/24

* DBSubnet (for DB Server): 10.0.2.0/24



10.0.0.0/16

10.0.0.0 /16

10.0.0.0 - 10.0.255.255 65,536 addresses

Subnets	IP address range	Size	NAT gateway
websubnet	10.0.0.0 - 10.0.0.255	/24 (256 addresses)	-
Appsubnet	10.0.1.0 - 10.0.1.255	/24 (256 addresses)	-
Dbsubnet	10.0.2.0 - 10.0.2.255	/24 (256 addresses)	-

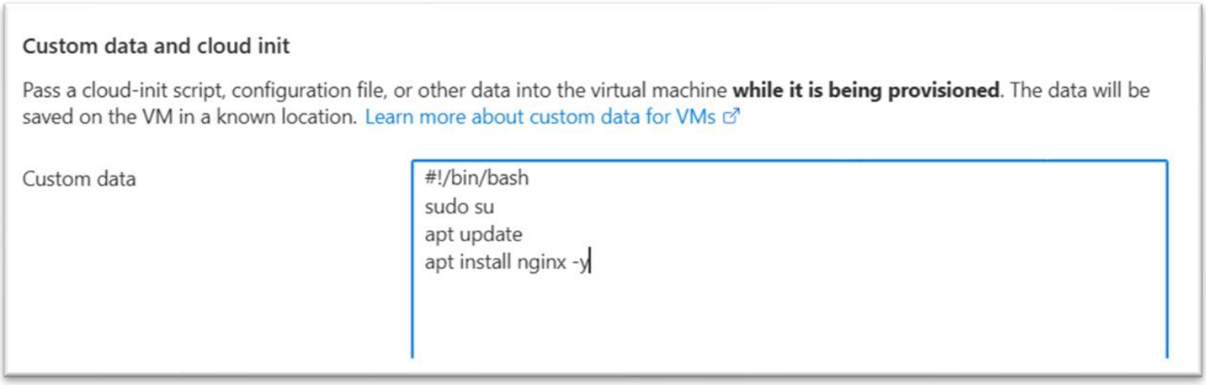
Step 3 – Create Three virtual machines:-

- Web-VM - (Install Nginx)
- App-VM - (Install Tomcat)

- Db-VM - (Install MySQL)

Install nginx in Web-VM:-

When we create web Virtual machine, we can install nginx software by writing custom data in advanced setting



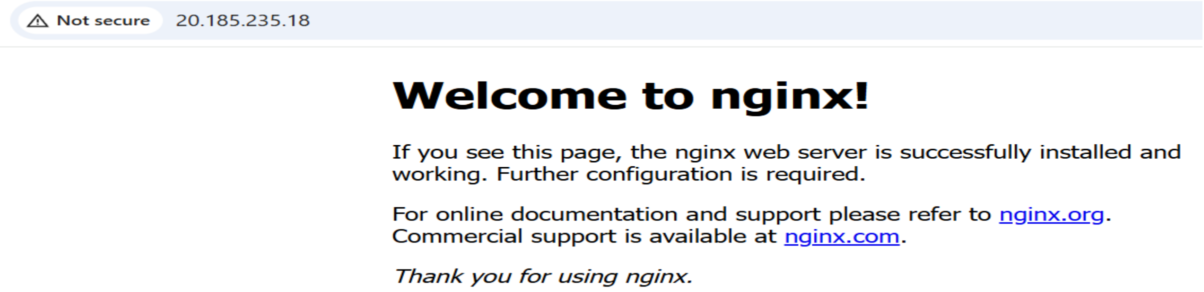
Custom data and cloud init

Pass a cloud-init script, configuration file, or other data into the virtual machine **while it is being provisioned**. The data will be saved on the VM in a known location. Learn more about custom data for VMs

Custom data

```
#!/bin/bash
sudo su
apt update
apt install nginx -y
```

Then you see this page on browser by navigating web IP address



Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org. Commercial support is available at nginx.com.

Thank you for using nginx.

Install tomcat in App-VM:-

Login into ubuntu machine

Step 1 : sudo apt update

Step 2 : sudo apt install default-jdk

Step 3 : java -version (in order to check whether the java is installed or not)

Step 4 : cd /opt/ (inside this folder create a tomcat directory)

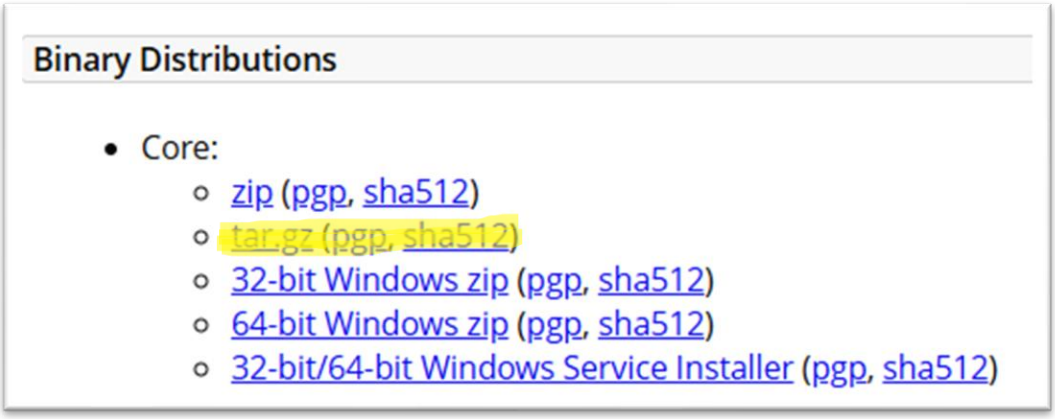
Step 5 : sudo mkdir tomcat

Step 6 : cd ..

Step 7 : cd /tmp/ (where we download the tomcat tar file)

To Download latest tomcat version, we go to browser and visit the https://tomcat.apache.org/

Copy the Highlighted URL



Binary Distributions

- Core:
  - zip (pgp, sha512)
  - tar.gz (pgp, sha512)
  - 32-bit Windows zip (pgp, sha512)
  - 64-bit Windows zip (pgp, sha512)
  - 32-bit/64-bit Windows Service Installer (pgp, sha512)

Step 8 : wget https://dlcdn.apache.org/tomcat/tomcat-10/v10.1.36/bin/apache-tomcat-10.1.36.tar.gz

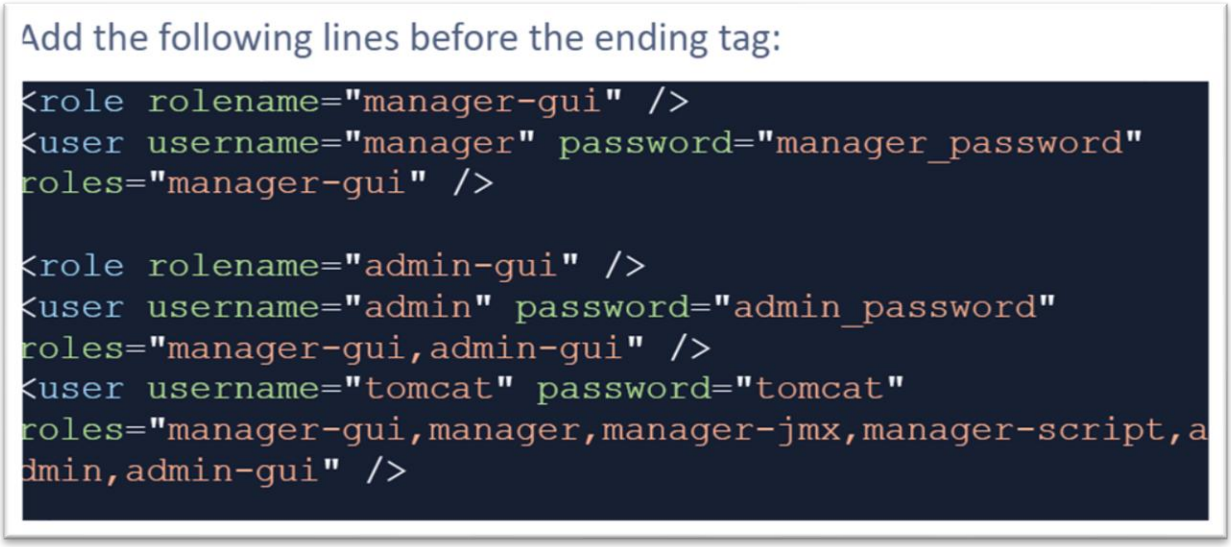
Step 9 : sudo tar xzvf apache-tomcat-10.1.36.tar.gz -C /opt/tomcat --strip-components=1(to unzip the tar file and move the contents of that file into previously created tomcat directory in opt)

Step 10 :sudo useradd -m -d /opt/tomcat -U -s /bin/false tomcat (Run the command to create a user called Tomcat)

Since you have already created a user, you can now grant tomcat ownership over the extracted installation by running:

1. sudo chown -R tomcat:tomcat /opt/tomcat/
2. sudo chomd -R u+x /opt/tomcat/bin

Step 11 : sudo nano /opt/tomcat/conf/tomcat-users.xml



Add the following lines before the ending tag:

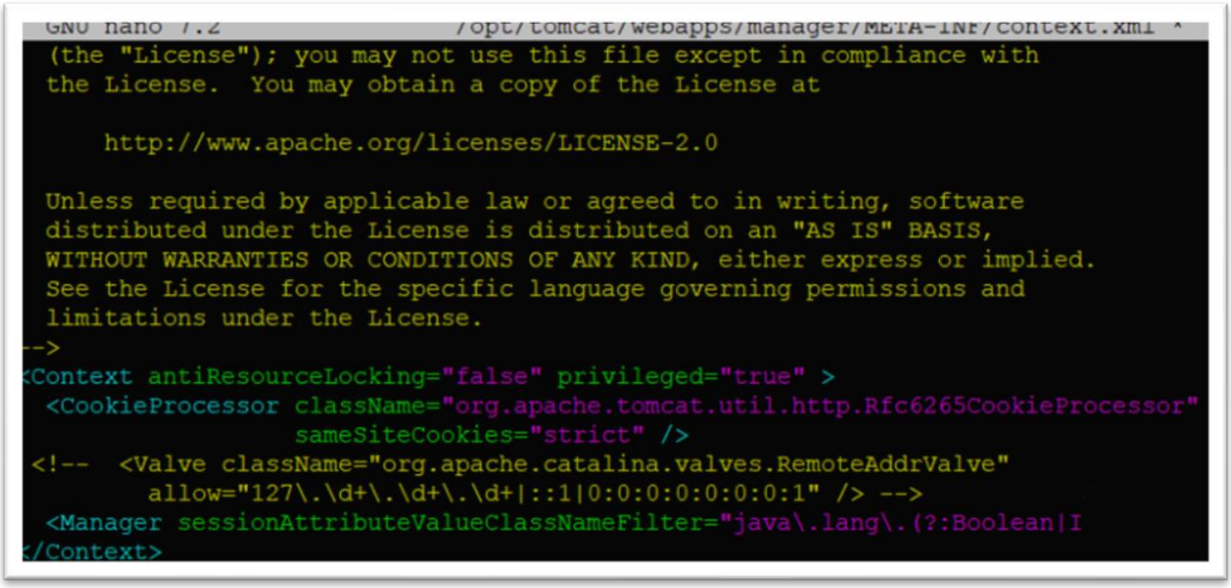
```
<role rolename="manager-gui" />
<user username="manager" password="manager_password"
roles="manager-gui" />

<role rolename="admin-gui" />
<user username="admin" password="admin_password"
roles="manager-gui,admin-gui" />
<user username="tomcat" password="tomcat"
roles="manager-gui,manager,manager-jmx,manager-script,a
dmin,admin-gui" />
```

Save the changes and **Exit** the file .

Step 12: sudo nano /opt/tomcat/webapps/manager/META-INF/context.xml

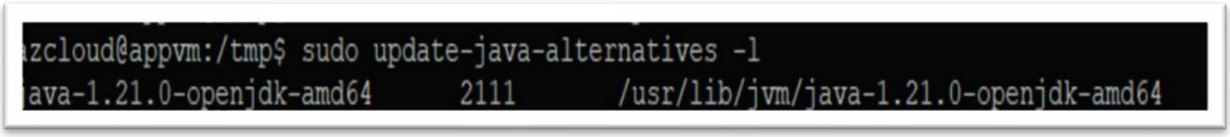
<!-- <Valve className="org.apache.catalina.valves.RemoteAddrValve"

allow="127\.\d+\.\d+\.\d+|::1|0:0:0:0:0:0:0:1" /> -->



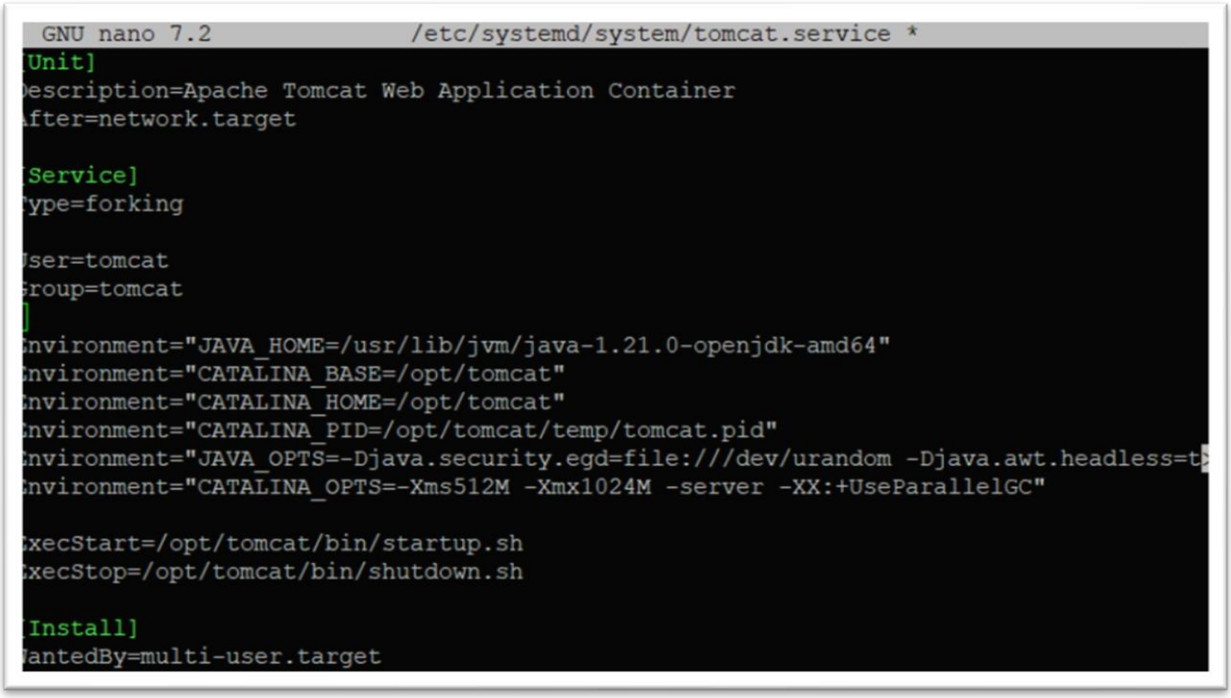
```
  GNU nano 7.2                 /opt/tomcat/webapps/manager/META-INF/context.xml *
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<Context antiResourceLocking="false" privileged="true" >
  <CookieProcessor className="org.apache.tomcat.util.http.Rfc6265CookieProcessor"
                   sameSiteCookies="strict" />
 <!--  <Valve className="org.apache.catalina.valves.RemoteAddrValve"
         allow="127\.\d+\.\d+\.\d+|::1|0:0:0:0:0:0:0:1" /> -->
  <Manager sessionAttributeValueClassNameFilter="java\.lang\.(?:Boolean|I
</Context>
```

Step 13: sudo update-java-alternatives -l



```
zcloud@appvm:/tmp$ sudo update-java-alternatives -l
ava-1.21.0-openjdk-amd64      2111       /usr/lib/jvm/java-1.21.0-openjdk-amd64
```

Step 14: sudo nano /etc/systemd/system/tomcat.service



```
 GNU nano 7.2                /etc/systemd/system/tomcat.service *
Unit]
escription=Apache Tomcat Web Application Container
fter=network.target

Service]
ype=forking

ser=tomcat
roup=tomcat

nvironment="JAVA_HOME=/usr/lib/jvm/java-1.21.0-openjdk-amd64"
nvironment="CATALINA_BASE=/opt/tomcat"
nvironment="CATALINA_HOME=/opt/tomcat"
nvironment="CATALINA_PID=/opt/tomcat/temp/tomcat.pid"
nvironment="JAVA_OPTS=-Djava.security.egd=file:///dev/urandom -Djava.awt.headless=t
nvironment="CATALINA_OPTS=-Xms512M -Xmx1024M -server -XX:+UseParallelGC"

xecStart=/opt/tomcat/bin/startup.sh
xecStop=/opt/tomcat/bin/shutdown.sh

Install]
antedBy=multi-user.target
```

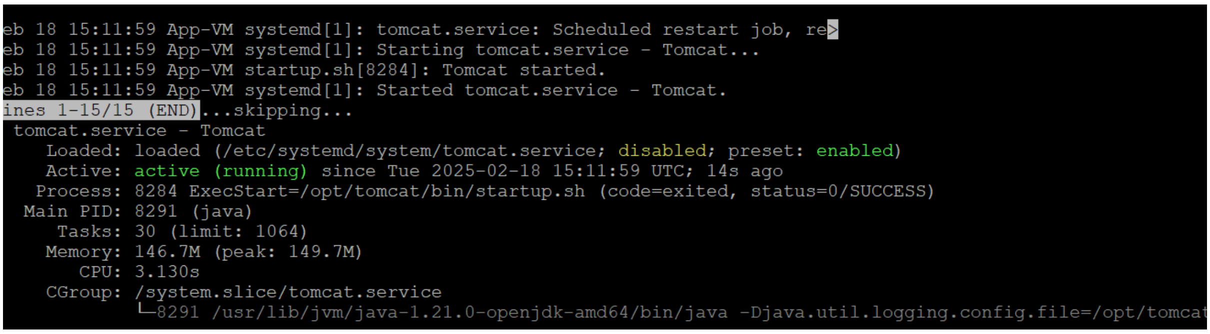
Save and **Exit** the file .

Step 15: sudo systemctl daemon-reload

Step 16: sudo systemctl start tomcat

Step 17: sudo systemctl enable tomcat

Step 18: sudo systemctl status tomcat

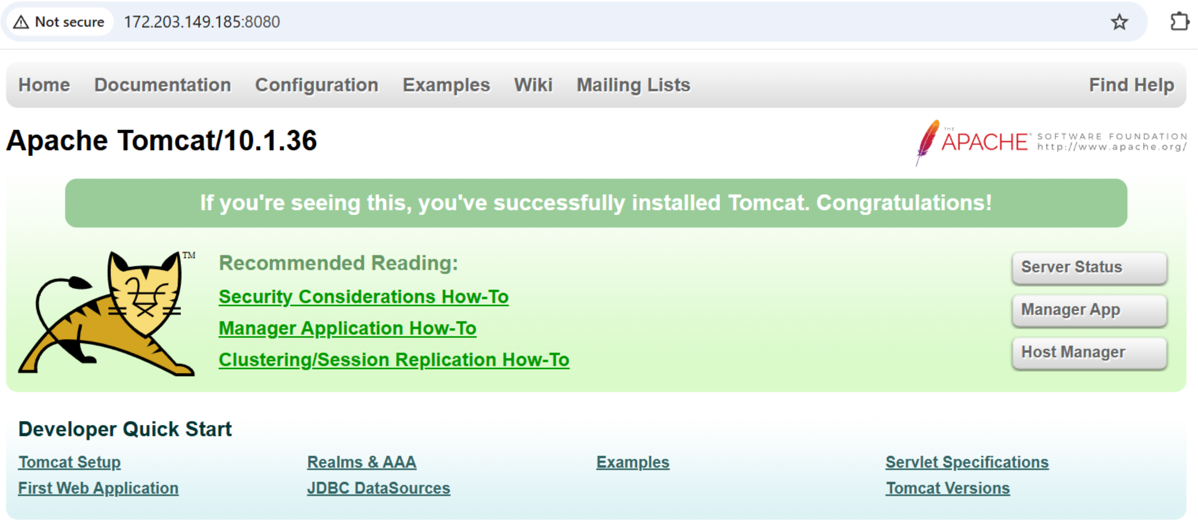


```
eb 18 15:11:59 App-VM systemd[1]: tomcat.service: Scheduled restart job, re>
eb 18 15:11:59 App-VM systemd[1]: Starting tomcat.service - Tomcat...
eb 18 15:11:59 App-VM startup.sh[8284]: Tomcat started.
eb 18 15:11:59 App-VM systemd[1]: Started tomcat.service - Tomcat.
ines 1-15/15 (END)...skipping...
 tomcat.service - Tomcat
    Loaded: loaded (/etc/systemd/system/tomcat.service; disabled; preset: enabled)
    Active: active (running) since Tue 2025-02-18 15:11:59 UTC; 14s ago
   Process: 8284 ExecStart=/opt/tomcat/bin/startup.sh (code=exited, status=0/SUCCESS)
  Main PID: 8291 (java)
     Tasks: 30 (limit: 1064)
    Memory: 146.7M (peak: 149.7M)
       CPU: 3.130s
    CGroup: /system.slice/tomcat.service
            └─8291 /usr/lib/jvm/java-1.21.0-openjdk-amd64/bin/java -Djava.util.logging.config.file=/opt/tomcat
```

Installations Completed

Now we can access tomcat in browser by navigating to IP address of our server:

http//: 172.203.149.185:8080/



Apache Tomcat/10.1.36

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Install MySQL in Db-VM :-

Install MY SQL DB on Linux machine using the below commands:

1. apt update —update the machine
2. apt install mysql-server -y ---- install my sql server
3. systemctl start mysql.service --- start the my sql server
4. systemctl status mysql ---- check the status whether it is in active &amp; running or not

5. systemctl enable mysql   ----- enable my sql in your system

6. mysql_secure_installation

7. y

8. y

9. 2

10. Y

11. Y

12. Y

13. y

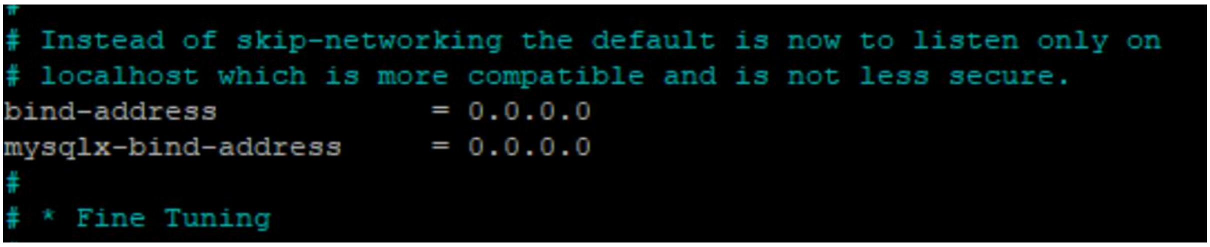
14. mysql   --- login into the mysql &amp; check the , exit
    from my sql

15. ctrl+z

16. nano /etc/mysql/mysql.conf.d/mysqld.cnf   -----◊edit the
    file as

(blind-address&amp- 0.0.0.0

mysqlx-blind-address- 0.0.0.0)



```
#
# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address            = 0.0.0.0
mysqlx-bind-address     = 0.0.0.0
#
# * Fine Tuning
```

After this do ctrl+x to save

Yes-y

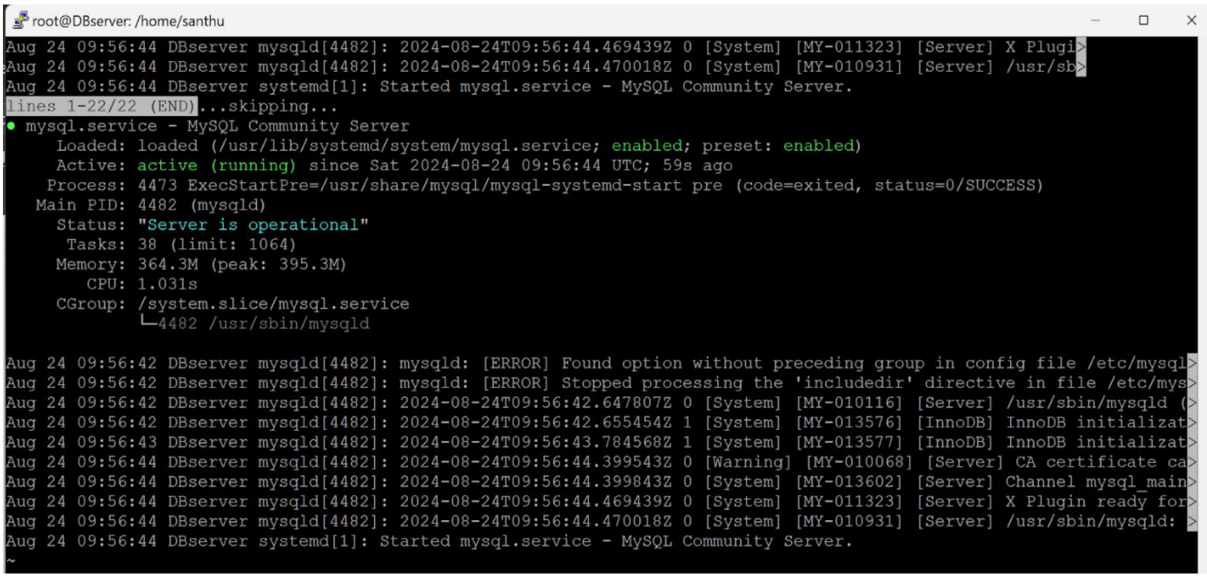
enter

17. systemctl restart mysql   -restart my sql

18. service mysql restart   -- restart my sql service

19. systemctl status mysql.service   --check the status

20. after successful installation you will be able to see the putty console like below



```
Aug 24 09:56:44 DBserver mysqld[4482]: 2024-08-24T09:56:44.469439Z 0 [System] [MY-011323] [Server] X Plugi>
Aug 24 09:56:44 DBserver mysqld[4482]: 2024-08-24T09:56:44.470018Z 0 [System] [MY-010931] [Server] /usr/sb>
Aug 24 09:56:44 DBserver systemd[1]: Started mysql.service - MySQL Community Server.
lines 1-22/22 (END)...skipping...
● mysql.service - MySQL Community Server
     Loaded: loaded (/usr/lib/systemd/system/mysql.service; enabled; preset: enabled)
     Active: active (running) since Sat 2024-08-24 09:56:44 UTC; 59s ago
    Process: 4473 ExecStartPre=/usr/share/mysql/mysql-systemd-start pre (code=exited, status=0/SUCCESS)
   Main PID: 4482 (mysqld)
     Status: "Server is operational"
      Tasks: 38 (limit: 1064)
     Memory: 364.3M (peak: 395.3M)
        CPU: 1.031s
     CGroup: /system.slice/mysql.service
             └─4482 /usr/sbin/mysqld

Aug 24 09:56:42 DBserver mysqld[4482]: mysqld: [ERROR] Found option without preceding group in config file /etc/mysql>
Aug 24 09:56:42 DBserver mysqld[4482]: mysqld: [ERROR] Stopped processing the 'includedir' directive in file /etc/mys>
Aug 24 09:56:42 DBserver mysqld[4482]: 2024-08-24T09:56:42.647807Z 0 [System] [MY-010116] [Server] /usr/sbin/mysqld (>
Aug 24 09:56:42 DBserver mysqld[4482]: 2024-08-24T09:56:42.655454Z 1 [System] [MY-013576] [InnoDB] InnoDB initializat>
Aug 24 09:56:43 DBserver mysqld[4482]: 2024-08-24T09:56:43.784568Z 1 [System] [MY-013577] [InnoDB] InnoDB initializat>
Aug 24 09:56:44 DBserver mysqld[4482]: 2024-08-24T09:56:44.399543Z 0 [Warning] [MY-010068] [Server] CA certificate ca>
Aug 24 09:56:44 DBserver mysqld[4482]: 2024-08-24T09:56:44.399843Z 0 [System] [MY-013602] [Server] Channel mysql_main>
Aug 24 09:56:44 DBserver mysqld[4482]: 2024-08-24T09:56:44.469439Z 0 [System] [MY-011323] [Server] X Plugin ready for>
Aug 24 09:56:44 DBserver mysqld[4482]: 2024-08-24T09:56:44.470018Z 0 [System] [MY-010931] [Server] /usr/sbin/mysqld: >
Aug 24 09:56:44 DBserver systemd[1]: Started mysql.service - MySQL Community Server.
~
```

Create Application Security Groups (ASG):-

a. Web ASG

- Group all VMs in the Web Subnet (i.e., WebServer VM) into a **Web ASG**.

b. App ASG

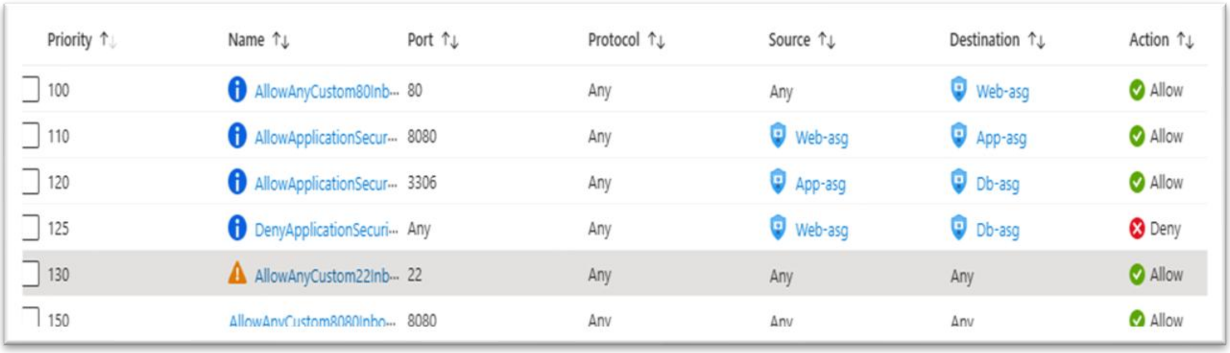
- Group all VMs in the app Subnet (i.e., AppServer VM) into a **app ASG**.

c. Db ASG

- Group all VMs in the Db Subnet (i.e., DBServer VM) into a **Db ASG**.

Then, Create Network Security Groups (NSG):-

Write these rules in NSG ;

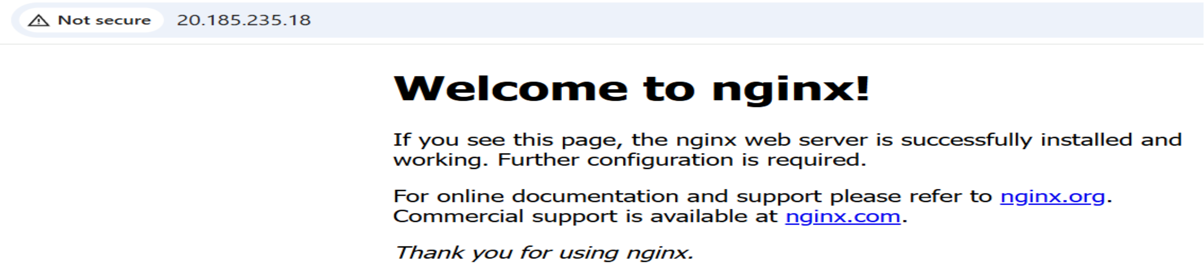


Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
□ 100	AllowAnyCustom80Inb...	80	Any	Any	Web-asg	✓ Allow
□ 110	AllowApplicationSecur...	8080	Any	Web-asg	App-asg	✓ Allow
□ 120	AllowApplicationSecur...	3306	Any	App-asg	Db-asg	✓ Allow
□ 125	DenyApplicationSecuri...	Any	Any	Web-asg	Db-asg	✗ Deny
□ 130	AllowAnyCustom22Inb...	22	Any	Any	Any	✓ Allow
□ 150	AllowAnyCustom8080Inbo...	8080	Any	Any	Any	✓ Allow

Attach all subnet to NSG .

RESULTS

1.Anyone should be able to access WEBVM on port 80 [it should be accessible in browser]



⚠ Not secure   20.185.235.18

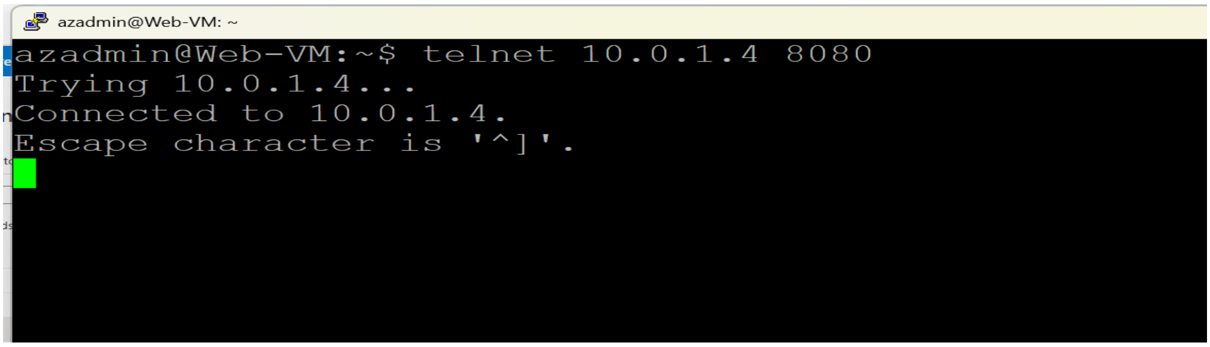
Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org. Commercial support is available at nginx.com.

Thank you for using nginx.

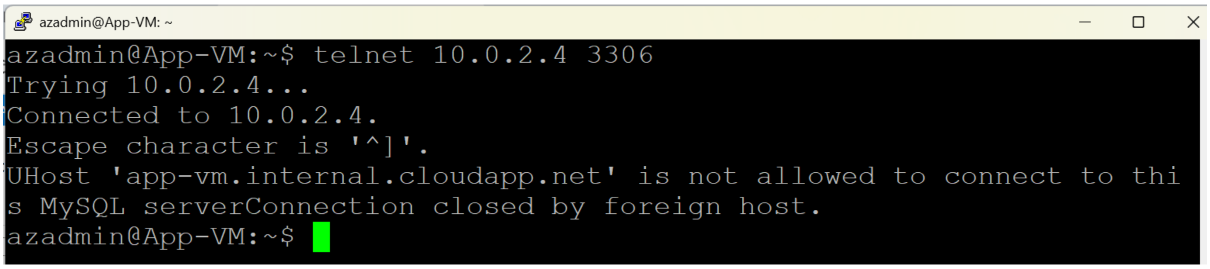
2.By using telnet command from WEBVM, Result should be able to get connect to APP-VM on port 8080 through WEBVM



azadmin@Web-VM: ~

```
azadmin@Web-VM:~$ telnet 10.0.1.4 8080
Trying 10.0.1.4...
Connected to 10.0.1.4.
Escape character is '^]'.
```

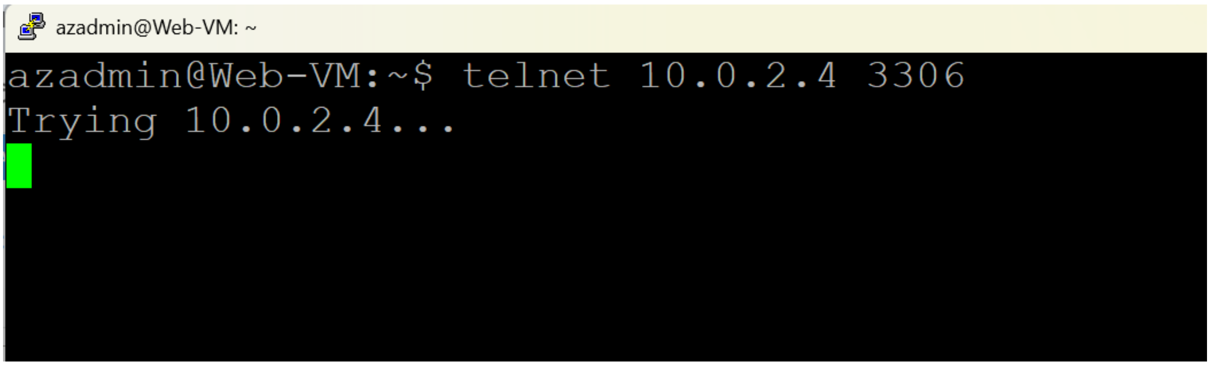
3.Telnet from APP-VM to DB-VM on port 3306/1433 result should be connected



```
azadmin@App-VM:~$ telnet 10.0.2.4 3306
Trying 10.0.2.4...
Connected to 10.0.2.4.
Escape character is '^]'.
UHost 'app-vm.internal.cloudapp.net' is not allowed to connect to thi
s MySQL serverConnection closed by foreign host.
azadmin@App-VM:~$
```

4.By using telnet command from WEB-VM, Result should not get connect to DB-VM on any port

Result → No Connection



```
azadmin@Web-VM:~$ telnet 10.0.2.4 3306
Trying 10.0.2.4...
```